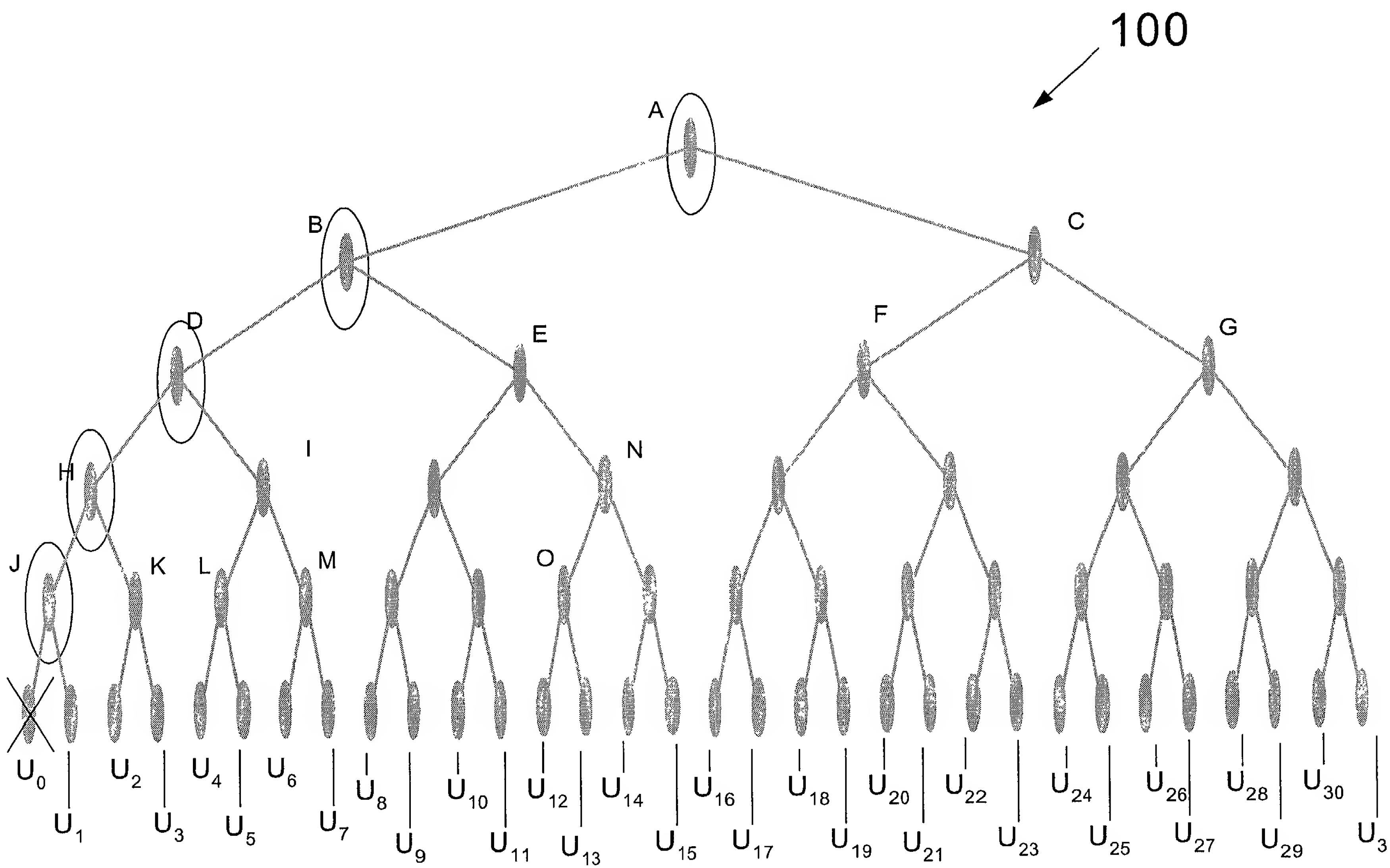

100
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
U0
U1
U2
U3
U4
U5
U6
U7
U8
U9
U10
U11
U12
U13
U14
U15
U16
U17
U18
U19
U20
U21
U22
U23
U24
U25
U26
U27
U28
U29
U30
U31

FIG. 1

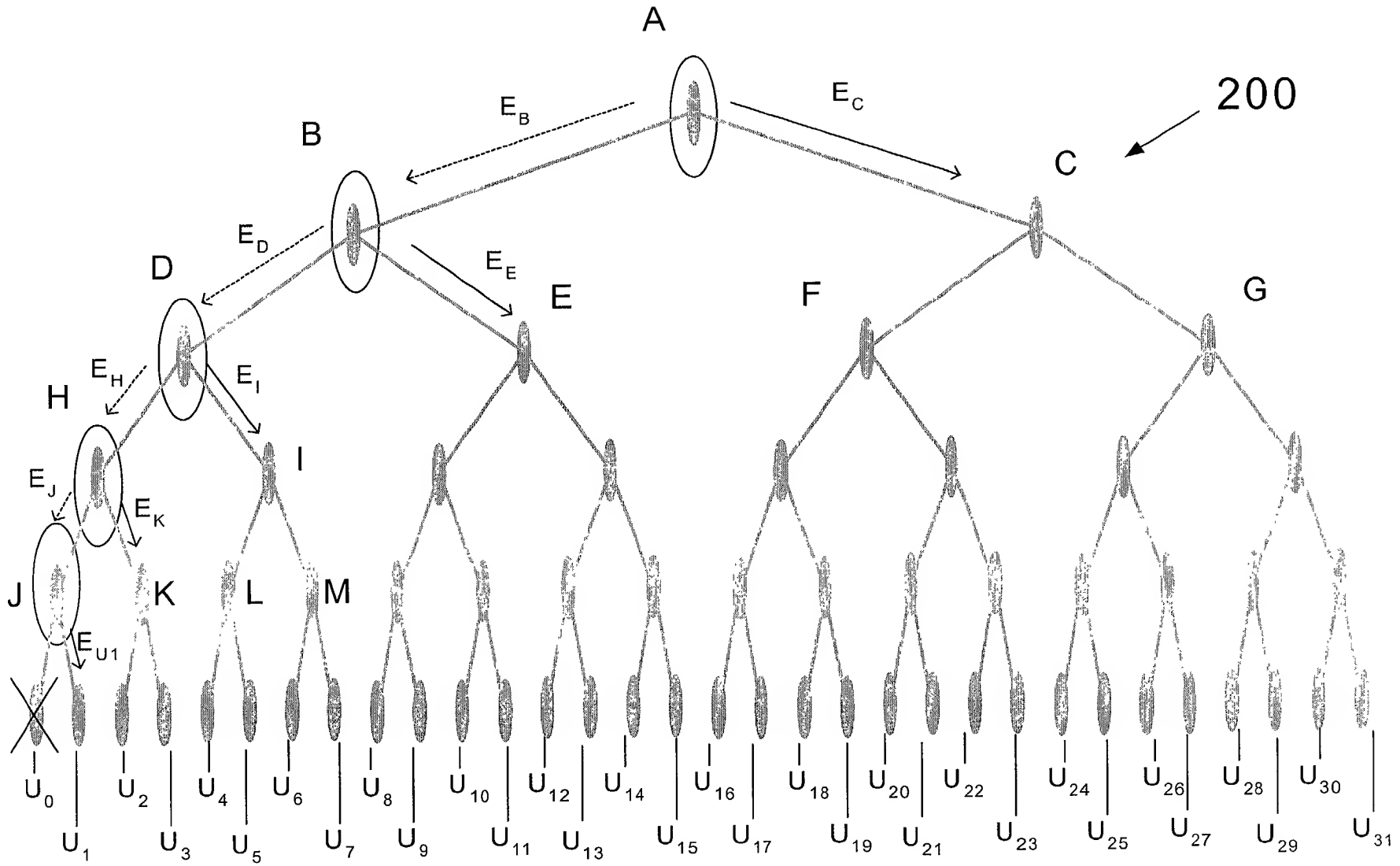


FIG. 2

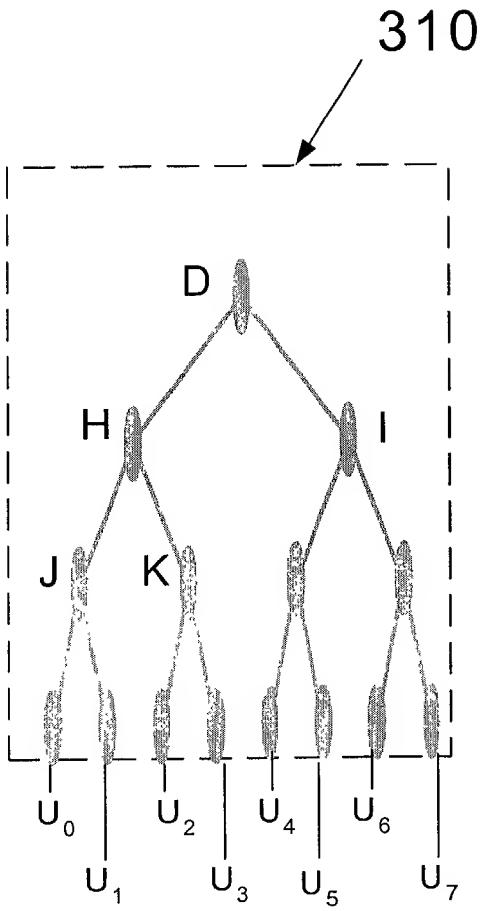


FIG. 3A

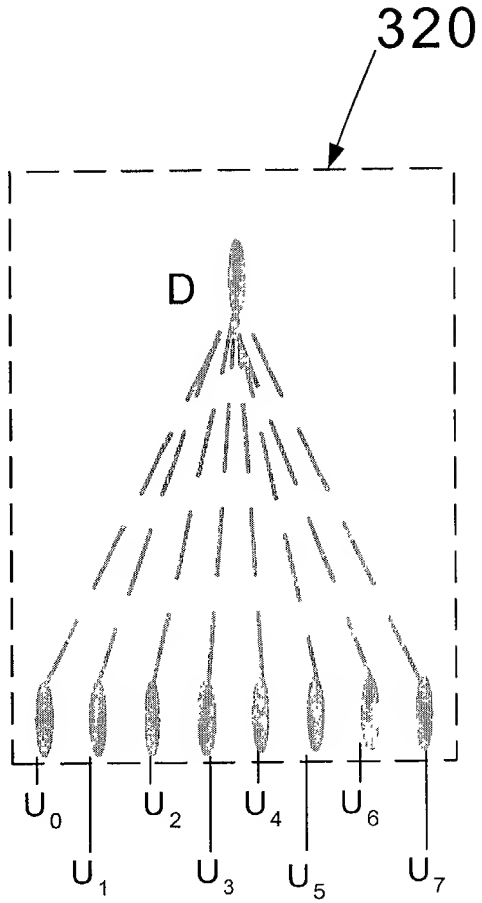


FIG. 3B

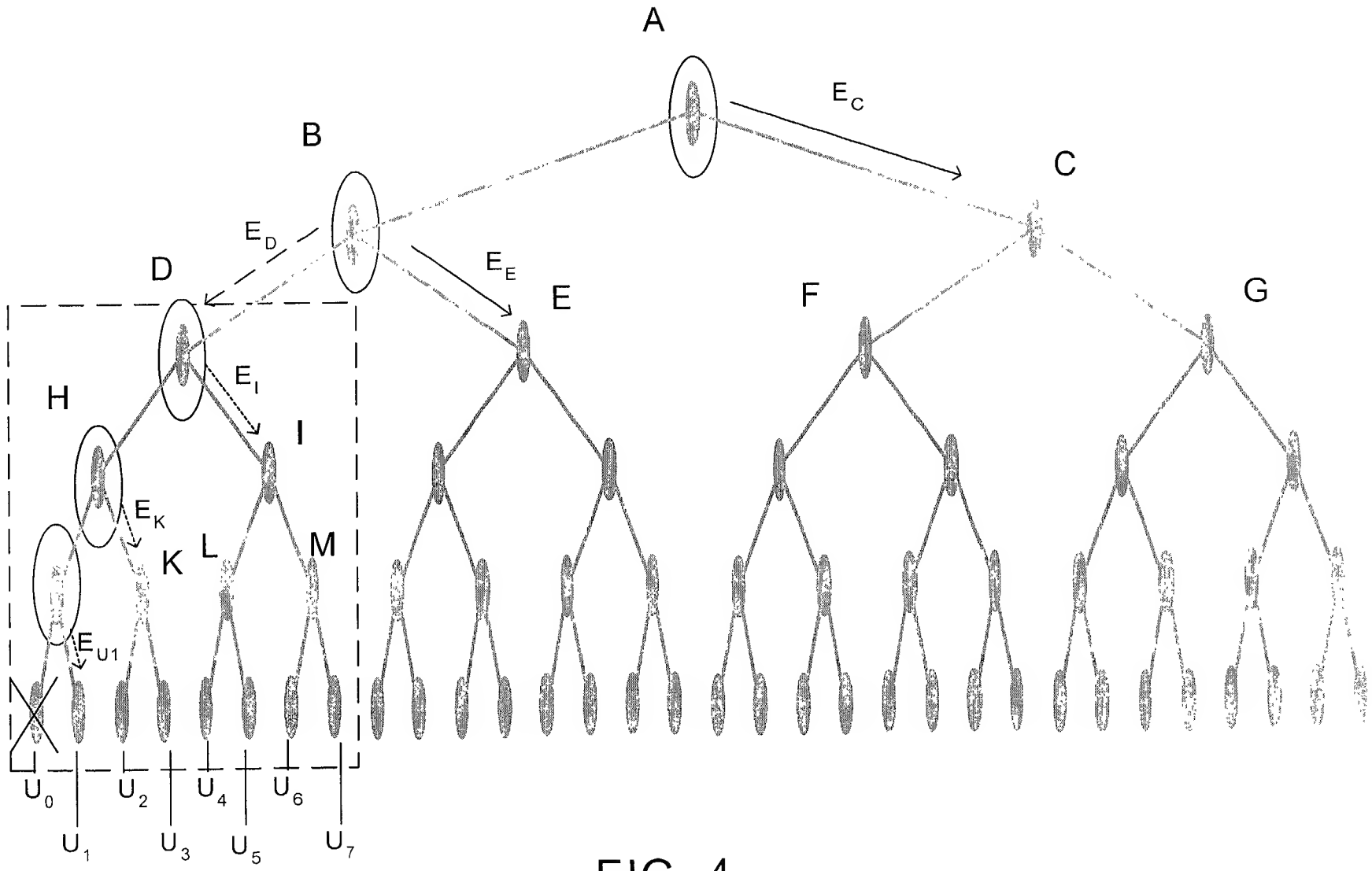


FIG. 4

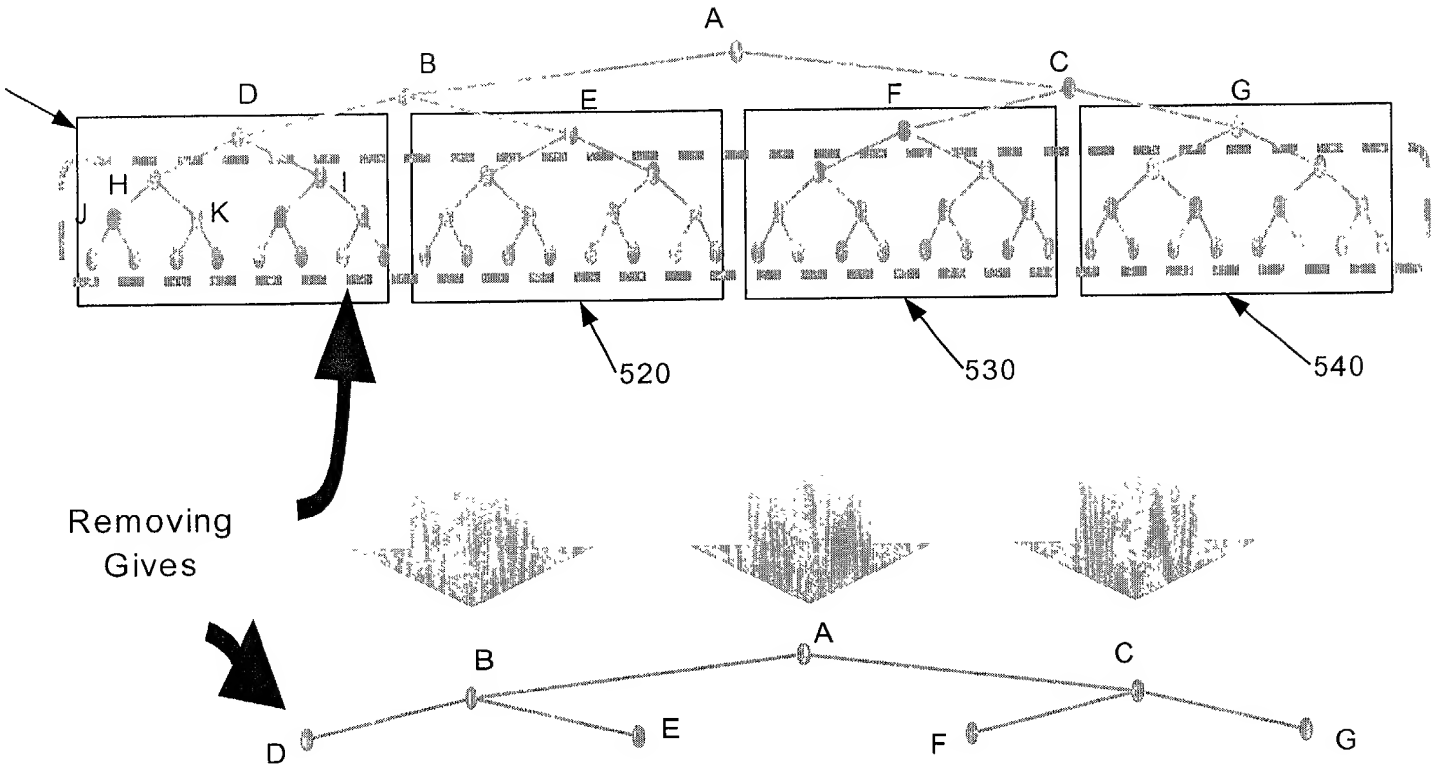


FIG. 5

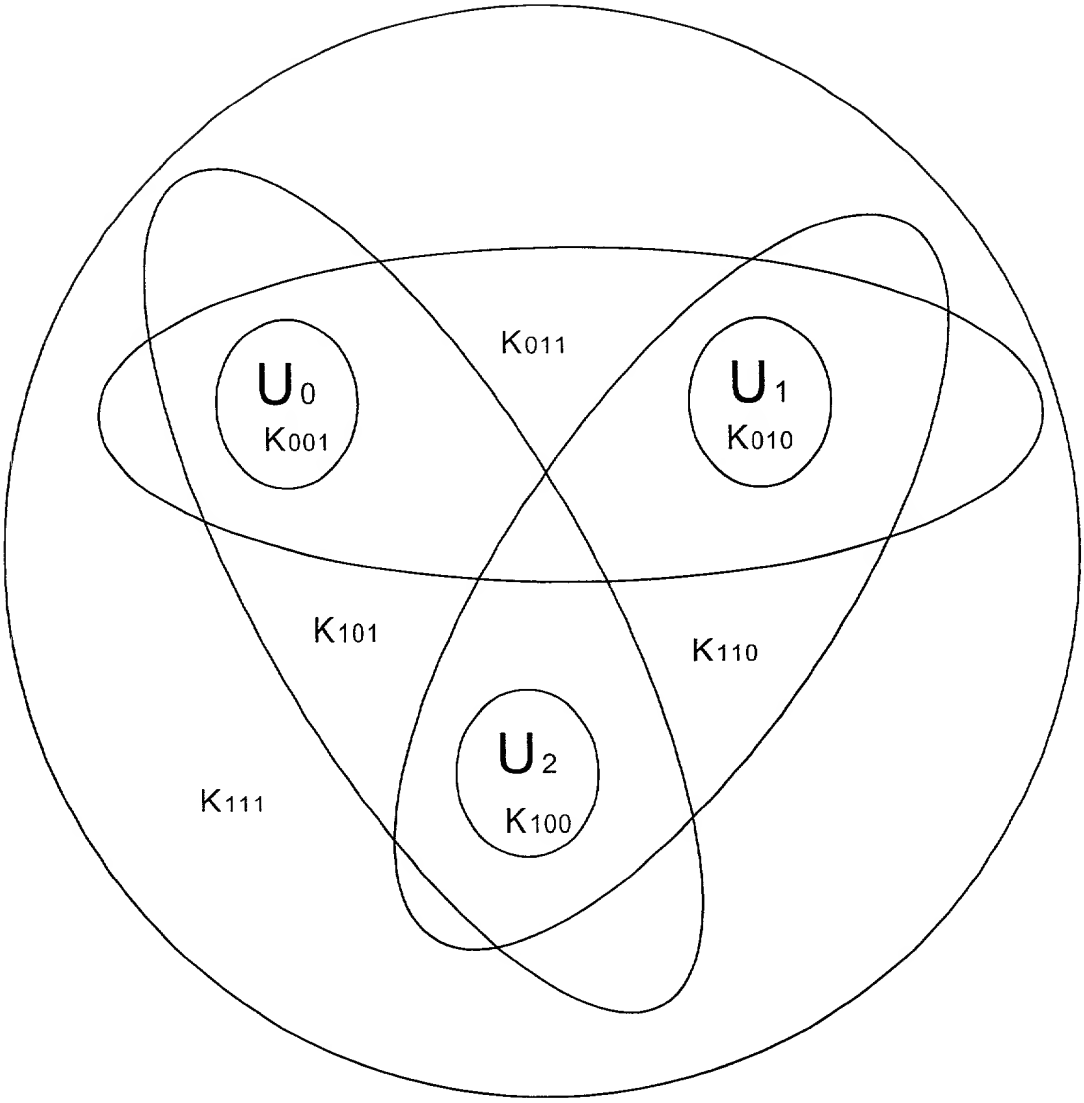


FIG. 6

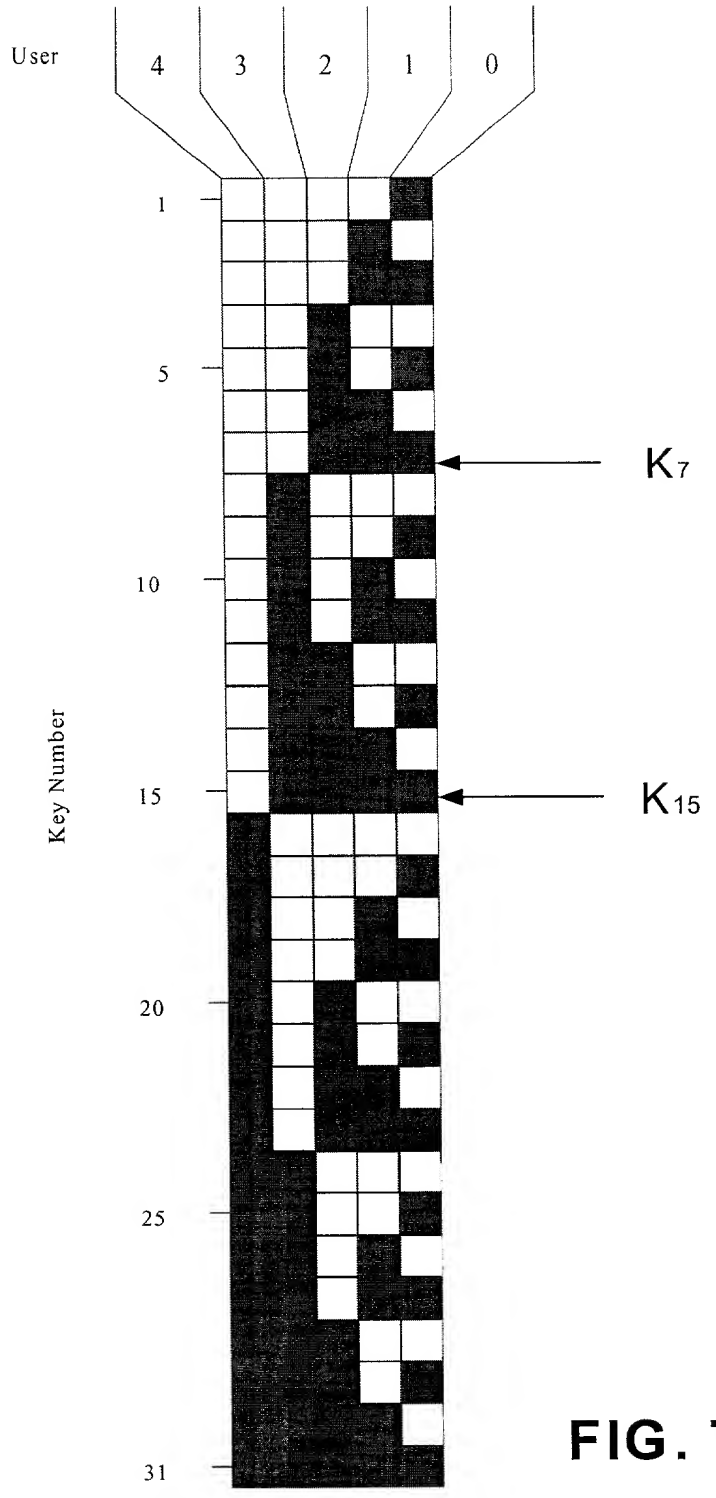


FIG. 7

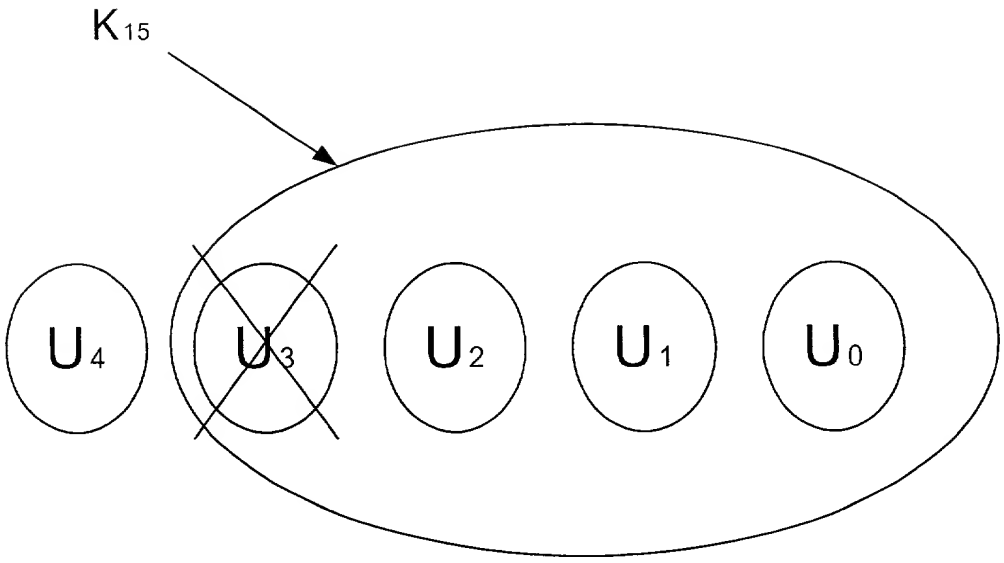


FIG. 8A

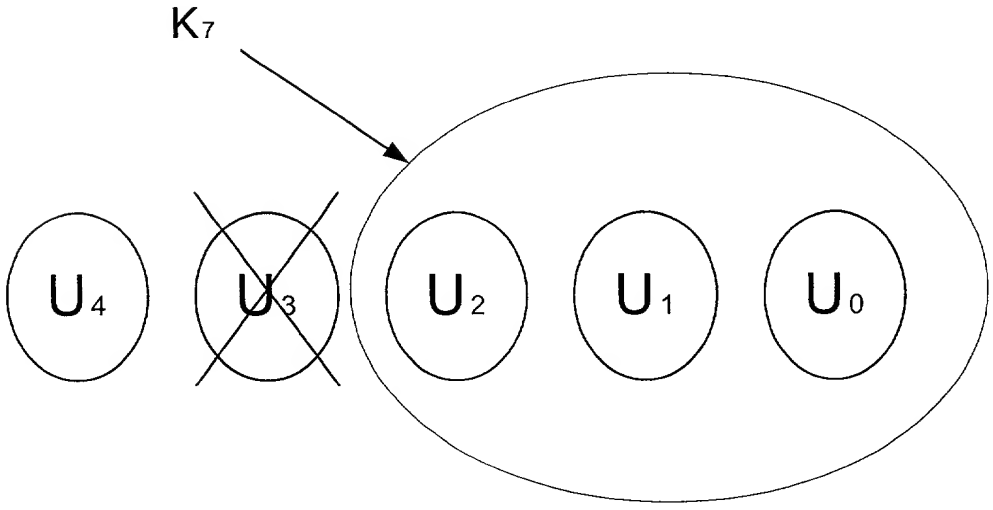


FIG. 8B

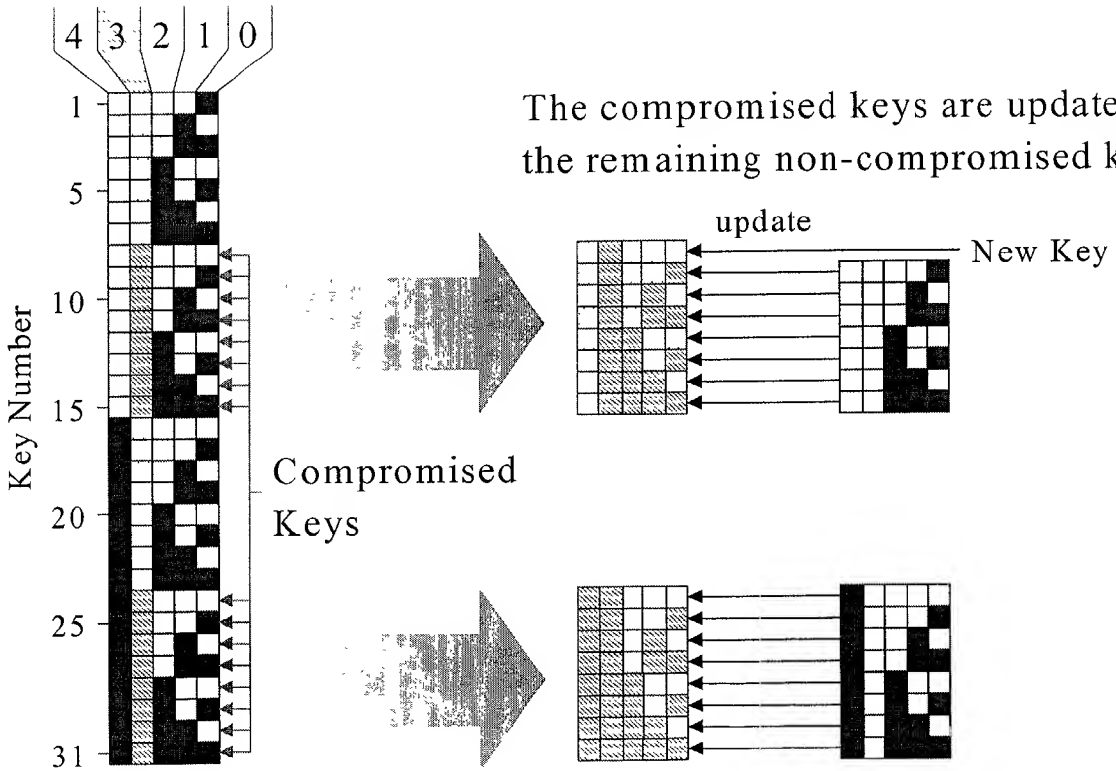

4
3
2
1
0
1
5
10
15
20
25
31
Key Number
Compromised Keys
The compromised keys are updated with the remaining non-compromised keys
update
New Key

FIG. 9

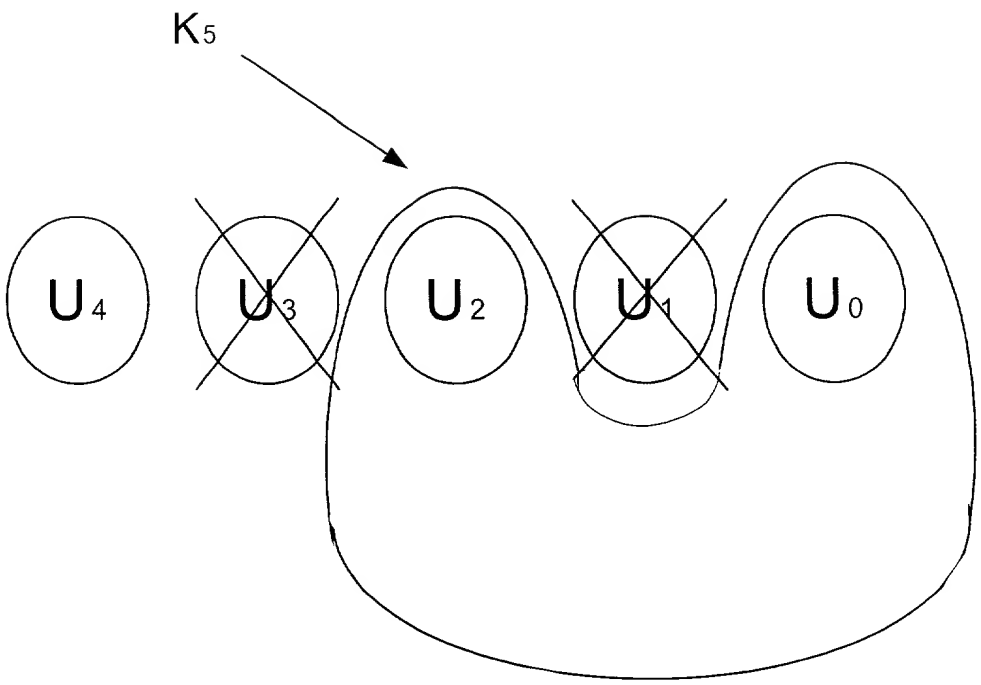


FIG. 10

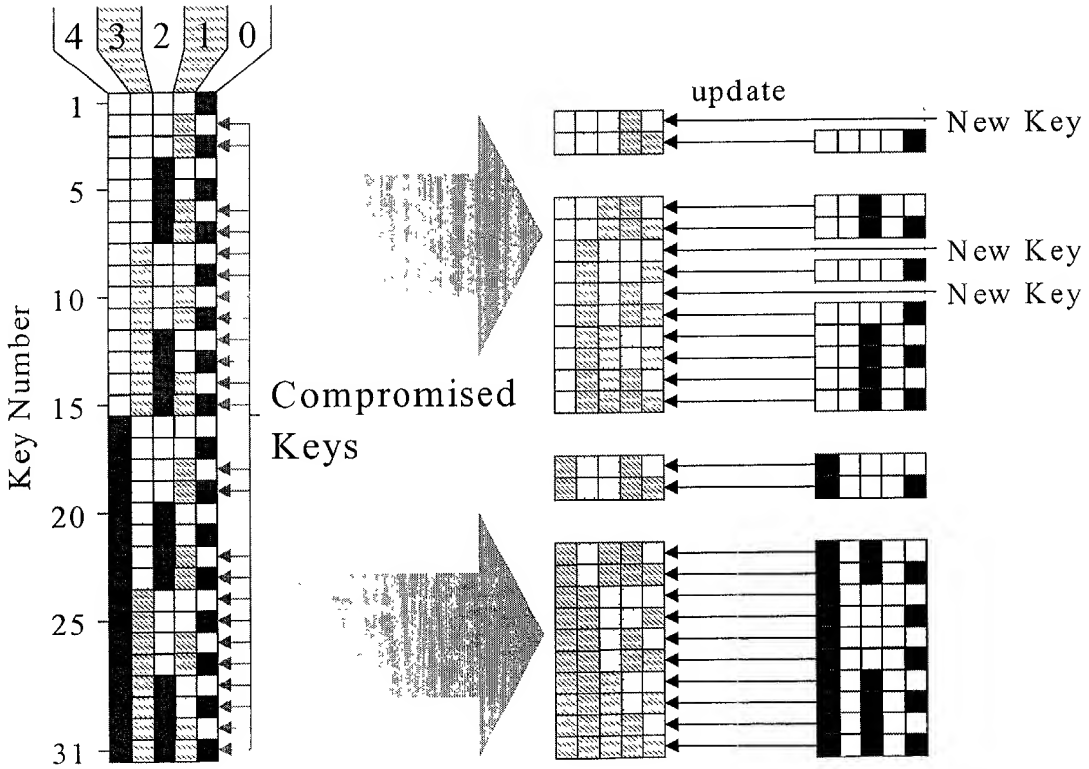

4
3
2
1
0
1
5
10
15
20
25
31
Key Number
Compromised Keys
update
New Key
New Key
New Key

FIG. 11

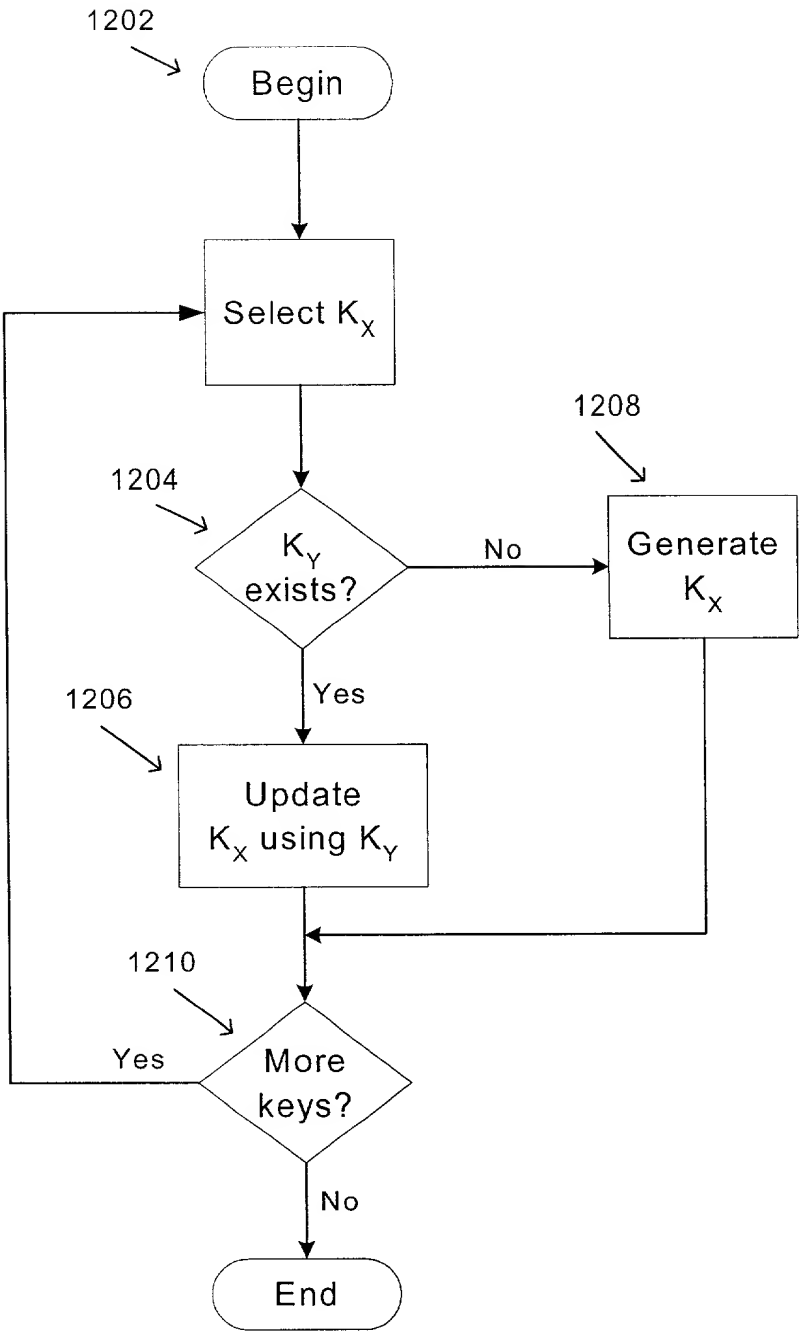
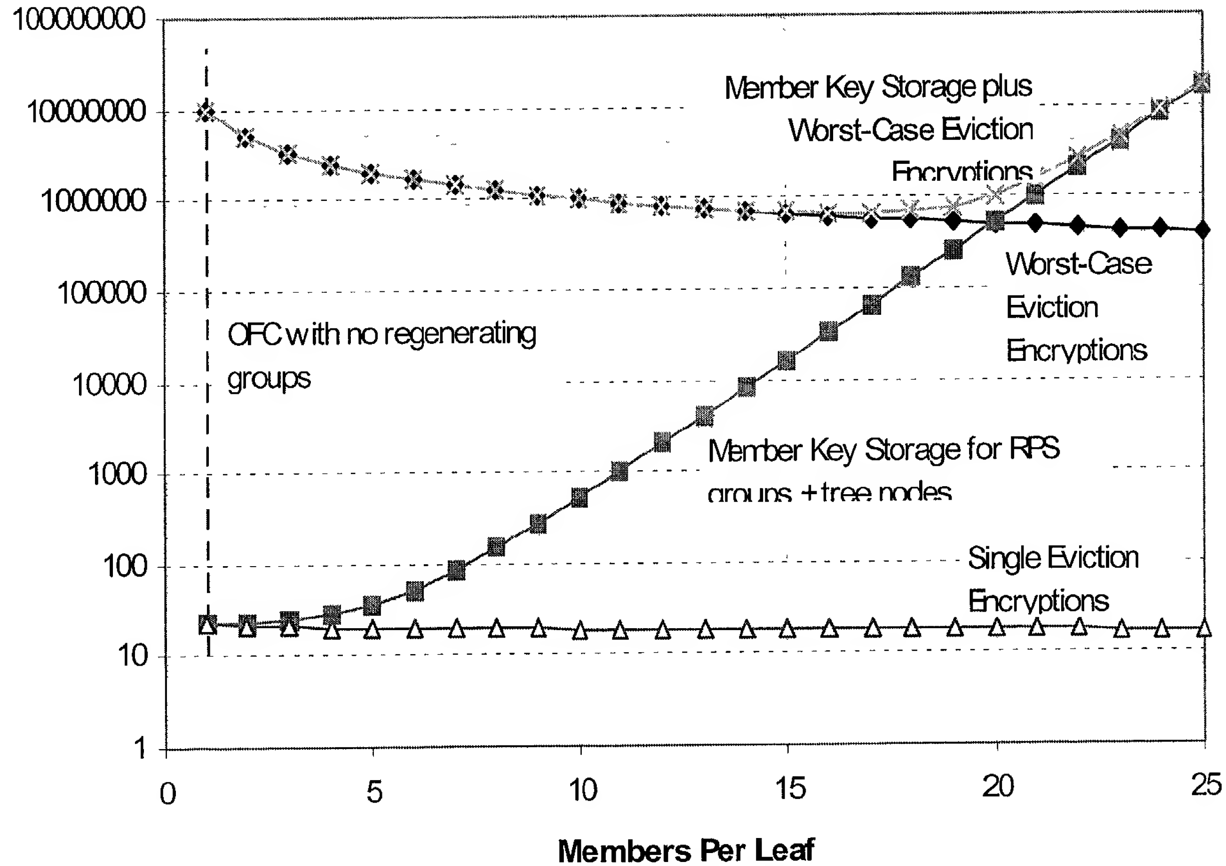

1202
Begin
Select K_X
1208
1204
K_Y exists?
No
Generate K_X
Yes
1206
Update K_X using K_Y
1210
Yes
More keys?
No
End

FIG. 12



100000000
10000000
1000000
100000
10000
1000
100
10
1
0
5
10
15
20
25
Members Per Leaf
Member Key Storage plus Worst-Case Eviction Encryptions
Worst-Case Eviction Encryptions
OFC with no regenerating groups
Member Key Storage for RPS groups + tree nodes
Single Eviction Encryptions

FIG. 13